**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Framework for Next Generation 911 Deployment | ) | PS Docket No. 10-255 |
| | ) | |
| | ) | |
| | ) | |

**To: The Commission**

**COMMENTS OF THE ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

*By its counsel:*

John A. Prendergast, Esquire

Blooston, Mordkofsky, Dickens,
Duffy & Prendergast, LLP
2120 L Street, NW, Suite 300
Washington, DC 20037
Tel. (202) 659-0830

Dated: February 28, 2011

## SUMMARY

AICC encourages the Commission to modify its proposed rules to allow Next Generation 911 calls using technologies where a high degree of adult human interaction prevents the sending of false, inadvertent, automated or malicious emergency calls. The Commission should refrain from facilitating the sending of alarm signals directly from alarm devices, security cameras and entertainment devices to the PSAP. Instead, the Commission should preserve the current arrangement whereby trained central station personnel screen alarm signals, to prevent a flood of false alarms to the already-overburdened PSAPs. Budget cuts and other circumstances have placed a tremendous strain on PSAPs. It is important not to create avenues for more 911 calls or messages that may be false or non-emergency, through the use of automatic equipment tied directly to the PSAP. The alarm industry has worked with public safety officials on an ongoing basis, to jointly develop protocols to weed out as many false alarms as possible. Through this joint effort, procedures have been established to identify and respond to most false alarms without having to utilize public safety resources. Without this screening, tens of thousands of false alarms could be sent by a single consumer-installed device, either maliciously or due to a malfunction or improper programming of the device. This volume of false 911 calls could effectively shut down many PSAPs for significant stretches of time, and expose PSAPs to greater risk of liability. Because of these dangers, many local ordinances prohibit the direct connection of automatic devices to the 911 system. Adding a 911 capability to entertainment devices used by children will only worsen the problem that could be caused by consumer alarm devices.

## TABLE OF CONTENTS

**SUMMARY** ..... ii

**TABLE OF CONTENTS** ..... iii

**I. Statement of Interest.** …….. .....2

**II. The Direct Transmission of Alarm Signals from Off-the-Shelf Devices to the PSAP Will Overwhelm State and Local Emergency Response Capabilities**.....3

**A. PSAPs are Already Under Tremendous Strain**……...4

**B. Direct Alarm Signals Can Flood a PSAP, Making it Impossible to Respond to Legitimate Emergencies**……5

1. **The alarm industry has worked hand in hand with public safety to develop false alarm protocols that drastically reduce false alarms**…….……..7

2. **Allowing direct connection of all IP enable alarm devices to the PSAP would expose public safety to "autodialer" problems**……..9

3. **False Signals Could Effectively Shut Down PSAPs, if Unscreened Alarm Signaling is allowed**……10

**C. Direct Alarm Signaling Can Significantly Increase Liability for PSAPs, Since They Lack a Contractual Relationship With the Callers**…….11

**D. The Proposal to Allow Security Cameras to Directly Contact a PSAP Raises Even More Issues**…….....12

**E. PSAPs Should Not Be Bombarded with 911 Signals from Televisions, iPods and Gaming Consoles**……..13

**III. The Commission Should Find That, on Balance, Direct 911 Calls From Consumer Alarm Systems, Security Cameras and Entertainment Devices Should Not be Allowed**……14

**CONCLUSION** .....15

**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Framework for Next Generation 911 Deployment | ) | PS Docket No. 10-255 |
| | ) | |
| | ) | |
| | ) | |

**To: The Commission**

**COMMENTS OF THE ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

*By its counsel:*

John A. Prendergast, Esquire

Blooston, Mordkofsky, Dickens,
Duffy & Prendergast, LLP
2120 L Street, NW, Suite 300
Washington, DC 20037
Tel. (202) 659-0830

Dated: February 28, 2011

## SUMMARY

AICC encourages the Commission to modify its proposed rules to allow Next Generation 911 calls using technologies where a high degree of adult human interaction prevents the sending of false, inadvertent, automated or malicious emergency calls. The Commission should refrain from facilitating the sending of alarm signals directly from alarm devices, security cameras and entertainment devices to the PSAP. Instead, the Commission should preserve the current arrangement whereby trained central station personnel screen alarm signals, to prevent a flood of false alarms to the already-overburdened PSAPs. Budget cuts and other circumstances have placed a tremendous strain on PSAPs. It is important not to create avenues for more 911 calls or messages that may be false or non-emergency, through the use of automatic equipment tied directly to the PSAP. The alarm industry has worked with public safety officials on an ongoing basis, to jointly develop protocols to weed out as many false alarms as possible. Through this joint effort, procedures have been established to identify and respond to most false alarms without having to utilize public safety resources. Without this screening, tens of thousands of false alarms could be sent by a single consumer-installed device, either maliciously or due to a malfunction or improper programming of the device. This volume of false 911 calls could effectively shut down many PSAPs for significant stretches of time, and expose PSAPs to greater risk of liability. Because of these dangers, many local ordinances prohibit the direct connection of automatic devices to the 911 system. Adding a 911 capability to entertainment devices used by children will only worsen the problem that could be caused by consumer alarm devices.

## TABLE OF CONTENTS

**SUMMARY** ..... ii

**TABLE OF CONTENTS** ..... iii

**I. Statement of Interest.** …….. .....2

**II. The Direct Transmission of Alarm Signals from Off-the-Shelf Devices to the PSAP Will Overwhelm State and Local Emergency Response Capabilities**.....3

**A. PSAPs are Already Under Tremendous Strain**……...4

**B. Direct Alarm Signals Can Flood a PSAP, Making it Impossible to Respond to Legitimate Emergencies**……5

1. **The alarm industry has worked hand in hand with public safety to develop false alarm protocols that drastically reduce false alarms**…….……..7

2. **Allowing direct connection of all IP enable alarm devices to the PSAP would expose public safety to "autodialer" problems**……..9

3. **False Signals Could Effectively Shut Down PSAPs, if Unscreened Alarm Signaling is allowed**……10

**C. Direct Alarm Signaling Can Significantly Increase Liability for PSAPs, Since They Lack a Contractual Relationship With the Callers**…….11

**D. The Proposal to Allow Security Cameras to Directly Contact a PSAP Raises Even More Issues**…….....12

**E. PSAPs Should Not Be Bombarded with 911 Signals from Televisions, iPods and Gaming Consoles**……..13

**III. The Commission Should Find That, on Balance, Direct 911 Calls From Consumer Alarm Systems, Security Cameras and Entertainment Devices Should Not be Allowed**……14

**CONCLUSION** .....15

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Framework for Next Generation 911 Deployment | ) | PS Docket No. 10-255 |
| | ) | |
| | ) | |
| | ) | |

**To: The Commission**

## COMMENTS OF THE ALARM INDUSTRY COMMUNICATIONS COMMITTEE

The Alarm Industry Communications Committee ("AICC"), on behalf of its members, submits these Comments in the above referenced proceeding, in which the Commission seeks information about how to best implement protocols to foster Next Generation 911 ("NG911") capabilities.[1] As discussed below, AICC supports the Commission's initiative to modernize the nation's 911 system, as there are technologies (such as texting) that can appropriately and effectively communicate with public safety dispatch centers. However, the Commission must recognize that, merely because a device is capable of communicating with public safety directly, does not mean that it should be so enabled. Otherwise, Public Safety Answering Points ("PSAPs") will be overwhelmed to the point of ineffectiveness, sorting through false alarms and automated signals that do not originate from actual emergencies.

[1] Notice of Inquiry ("NOI"), PS Docket No. 10-255, FCC 10-200, released December 21, 2010 [76 FR 2297, January 13, 2011].

## I. Statement of Interest

AICC is comprised of representatives of the Central Station Alarm Association (CSAA), Electronic Security Association (ESA),[2] Bosch Security Systems, Digital Monitoring Products, Digital Security Control, Telular Corp, Stanley Convergent (alarm division, formerly known as Honeywell Monitoring), Honeywell Security, Vector Security, Inc., ADT Security Services, Inc., AES- IntelliNet, Alarm.com, Bay Alarm, Intertek Testing, RSI Videofied, Security Network of America, United Central Control, Security Industry Association (SIA), AFA Protective Systems, Vivint (formerly APX Alarm), COPS Monitoring, DGA Security, Security Networks, Universal Atlantic Systems, Axis Communications, Interlogix, LogicMark, Napco Security, and the Underwriters Laboratories.

ESA and CSAA, representing the alarm dealer segment, have 2434 member companies providing alarm service to the public. AICC member companies protect a wide range of sensitive facilities and their occupants from fire, burglaries, sabotage and other emergencies. Protected facilities include government offices, power plants, hospitals, dam and water authorities, pharmaceutical plants, chemical plants, banks, schools and universities. In addition to these commercial and governmental applications, alarm companies protect a large and ever increasing number of residences and their occupants from fire, intruders, and carbon monoxide poisoning. Alarm companies also

[2] CSAA and ESA are associations comprised of central station alarm companies, alarm monitoring centers, alarm installation companies and alarm manufacturing companies. Their memberships represent the majority of such companies operating in the United States.

provide medical alert services for obtaining ambulances in the event of medical emergencies.

The alarm industry works hand in hand with the public safety community to identify ways to best relay information about genuine emergencies requiring a PSAP response, while limiting the burden on public safety resources through a screening of false alarms and non-emergency events.

## II. The Direct Transmission of Alarm Signals from Off-the-Shelf Devices to the PSAP Will Overwhelm State and Local Emergency Response Capabilities.

In the NOI in this proceeding, the Commission asks whether and how it should foster "device initiated services for emergency communications". In particular, paragraph 58 of the NOI asks whether alarm systems and security cameras (among other devices) should be able to directly contact PSAPs to initiate 911 calls:

> *58. Device-Initiated Services for Emergency Communications.* In an IP-based network architecture, emergency calls can be placed not only by human beings, but by a variety of automatically triggered devices. Examples of such devices include environmental sensors capable of detecting chemicals, highway cameras, *security cameras, alarms*, personal medical devices, telematics, and consumer electronics in automobiles. We seek comment on how the deployment of NG911 will facilitate the ability of device-initiated emergency services to reach PSAPs. What steps are needed to facilitate such deployment? [*Emphasis added*]

The concept of having alarm devices communicate directly with the PSAP has a certain theoretical appeal. However, as described below, the experience of the alarm industry and the public safety community provides direct evidence that this arrangement would have a disastrous effect on the ability of PSAPs to respond to emergencies.

### A. PSAPs are Already Under Tremendous Strain

Cellular telephone service has proven to be an invaluable tool to public safety. Motorists and pedestrians are now able to report real time eyewitness accounts of accidents, fires, crimes and other events requiring an emergency response. As valuable as this capability has become, it has also placed a significantly greater burden on PSAPs. First, the increased volume of legitimate emergency calls has significantly added to the burden on 911 dispatchers. Of course, this aspect of cellular service is welcomed, because it represents live human beings reporting incidents to the appropriate public safety agencies. However, even with the human intervention element associated with cell phone use, this technology has added to the significant unnecessary burden already experienced by PSAPs. As reported in the U.S. Department of Justice study entitled "Misuse and Abuse of 911"[3], the several issues exist from wireline and wireless telephone calls to 911, including phantom calls,[4] misdials, and intentional non-emergency calls (such as prank calls, exaggeration calls by persons wanting faster public services, and "lonely complainant" calls). *Id.* at pp.4-6.

The wireless industry is working with the public safety community to address the burden on PSAPs, but even as they make progress, budget cuts and other circumstances have preserved the strain on PSAPs that has existed now for decades. See, e.g., "911 Emergency System Overtaxed, Study Says", Chicago Tribune, June 4, 1987;

---

[3] U. S. Department of Justice, "Misuse and Abuse of 911- Problem-Oriented Guides for Police", Rana Sampson, August 2004 (available at www.cops.usdoj.gov).

[4] The "phantom calls" category includes 911 calls placed by a cell phone user that inadvertently presses the 9 or 1 key on a phone preprogrammed to dial 911, even if the user does not press "send". The National Emergency Number Association (NENA) has reported that phantom wireless calls have accounted for between 25 and 70 percent of all 911 calls in some U.S. communities. Id. at p. 3. The California Highway Patrol estimates that between 1.8 million and 3.6 million of the 6 million wireless 911 calls it receives annually are phantom. Id.

"Overworked 911 Center Cited in Delayed Fire Response", Eric Stirgus, The Atlanta Journal-Constitution, January 28, 2009 ("The public safety system in Atlanta is stretched to the breaking point."); "Increase In Cell Phone Calls Burden 911 Centers", NBC13.com, February 15, 2005; "Number of 911 Calls Keeps Rising", Brennan David, the Columbia Daily Tribune, January 11, 2011.

The usual strain on PSAPs is exacerbated by widespread emergency events, such as snow or ice storms, terrorist attacks, or even public demonstrations/rallies. See "Unusual 911 Calls Flooded FDNY During Blizzard", Ginger Adams Otis, The New York Post, January 13, 2011 ("A backlog of emergency calls built up overnight on Sunday, Dec. 26, as nearly two feet of snow got dumped on the city, and by the following morning city officials were begging residents to reserve 911 for life-threatening situations.") In light of this dynamic, it is important not to create avenues for more 911 calls or messages that may be false or non-emergency, through the use of automatic equipment tied directly to the PSAP.

**B. Direct Alarm Signals Can Flood a PSAP, Making it Impossible to Respond to Legitimate Emergencies.**

As is the case with cellular service, the use of alarm systems to signal for help has proven to be a vital avenue for saving lives and property. The detection of fires, home invasions and medical emergencies through the use of alarm devices has saved untold numbers of lives, and prevented even greater harms to society as an emergency is contained and an appropriate response sent (especially in the case of fires). However, unlike cellular calls, most alarm signals are not instigated through human intervention, but instead are the result of a sensor automatically detecting what is perceived to be an emergency condition and sending a digital signal. With the exception of "panic button"

alerts (where the alarm customer presses a button that alerts the alarm monitoring center that a witnessed emergency is occurring), there may be no overt action by a human being when an alarm signal is sent. Of course, in the event of an actual emergency, the automatic sending of this signal is vital when, e.g., the occupants of a house are overcome by carbon monoxide and cannot trigger the alarm for themselves. However, the use of automatic alarm signals also creates the possibility that a false alarm signal has been sent. Examples of common false alarms include:

- Failure of the user to leave their premises before the alarm exit delay expires.
- Failure of the user to secure/close/lock all windows and doors before arming the alarm system, and the wind blows a door open.
- Leaving pets in open areas where motion detectors are in operation, or failure to turn off motion detectors when animals or people are present.
- Failure of a person entering a protected premises to deactivate the system within the prescribed delay period.
- Entering or exiting a premise through a non-delayed or immediate alarm coded zone, such as a basement door.
- Failure to secure/remove moving objects in a zone with motion detection (e.g., a Mylar balloon, or a hanging display sign that moves when an air handler turns on).
- Inadvertent activation of manual buttons on wireless remote controls or hold-up/panic switches in fixed locations by people unfamiliar with their system, or juveniles.
- Operation of a main security system or associated fixed or wireless devices by untrained users.
- Failure by users to properly maintain or service equipment, e.g. repeated use of a system with faulty sensors.

Responding to false alarms can place a significant burden on PSAPs and first responders. Alarm monitoring companies work to overcome this problem by screening virtually all alarm signals, using personnel trained in the strict procedures involved in

obtaining certification of the central station by Underwriters' Laboratories or one of the other nationally-recognized rating agencies prescribed by Section 90.35(c) of the Commission's Rules.[5] The central station personnel (1) arrange for an emergency response by public safety personnel if an emergency is confirmed; (2) contact the customer if the nature of the alarm signal cannot be readily established; and (3) identify false alarms using established procedures, so that public safety resources are not wasted on this task.

**1. The alarm industry has worked hand in hand with public safety to develop false alarm protocols that drastically reduce false alarms.**

In response to the significant number of false alarms that began to occur as residential use of alarm systems flourished, the alarm industry met with public safety officials on an ongoing basis, to jointly develop protocols to weed out as many false alarms as possible. Through this joint effort, procedures have been established to identify and respond to most false alarms without having to utilize public safety resources. The alarm industry has found that, using these procedures, it is able to avoid sending a public safety response to approximately 93 percent of all alarm signals, either because the signals constituted false alarms or because the central station personnel were able to direct the customer as to how to handle their situation. Often, the central station can dispatch private security guards to investigate a situation, again lightening the burden on public safety.

[5] Certain alarm signals involving the reporting of a fire in a commercial property can be sent directly to the PSAP by prior arrangement. However, this arrangement is being re-examined in connection with the updating of National Fire Protection Association (NFPA) Code 72, at the urging of the International Association of Fire Chiefs (IAFC). An examination of 10,000 direct fire alarms involved less than ten calls that required an emergency response, indicating that screening by the central station would be beneficial.

In particular, the alarm industry has worked closely with the International Association of Chiefs of Police (IACP) and other public safety agencies, to develop protocols such as those embodied in the ANSI/CSAA CS-V-01 standard (formulating the Enhanced Call Verification standard, with input from public safety officials and insurance industry representatives) and ANSI SIA MSD-01-1999.06 standard (mobile security device protocol formulated and voted on by a standards committee that included IACP and representatives of several police departments, as well as alarm company and manufacturer representatives). Under these protocols, data alarm messages are not turned into a PSAP request for response until there has been an attempt by trained central station personnel to verify that an emergency situation exists, and appropriate information for the PSAP is obtained. The techniques that are most successful and are promoted for effective reductions are embodied in the alarm industry's False Alarm Screening "Best Practices" guidelines, including such measures as:

- Two-call verification or Enhanced Call Verification (ECV), where the monitoring center makes two calls to separate phone numbers (one typically a cellphone) in an attempt to determine the validity of the need for PSAP notification/dispatch.
- Video or Audio confirmation requirement for PSAP contact, determined with proprietary guidelines established for operators by each monitoring center.
- Software automation that under appropriate circumstances processes a verified "cancel" signal from the premises prior to the monitoring center operator completing the call to a PSAP.
- A hardware/software solution that processes a cancellation at the premises, but still allows monitoring center notification for the purpose of servicing faulty equipment.
- Hardware/software solutions built into the alarm equipment, using the ANSI/SIA CP-01 2010 standard, which corrects/compensates for common user errors at the user location.
- Multiple alarm zone trip counting/verification by central station personnel in cases where users have a propensity for false alarms.

- Use of an acclimation period for new customers, where a central station uses special procedures in processing any alarm signal from a new alarm system for a period (typically seven days), to allow the new user(s) time to practice/familiarize themselves with the new system.

Even with the above protocols, the false alarm problem is not entirely eliminated, but the situation is made manageable. If all alarm signals were sent to PSAPs unscreened, there would be an 1100% increase in alarm signal calls to which the PSAPs would have to respond. If the public is allowed to directly send alarm signals to PSAP with any device that has an IP capability, it would be akin to telling alarm carriers to stop screening alarms signals; except it is estimated that there would be a geometric increase in signals sent, over and above the 1100% increase that would be represented by those alarms that are already being screened out by the central stations alarm service providers. This is due in part to the fact that the alarm signals already screened out by central station personnel are generated by alarm systems that have been professionally installed, and operator error is the most common cause of the false alarm. If millions of consumers install alarm devices themselves, there will be the usual number of operator-error false alarms generated by such devices, plus a significant number of false alarms due to faulty installation. The mere failure to properly install a back up power source will cause a number of alarm devices to send an alarm signal whenever power is interrupted. It is also foreseeable that the number of operator error false alarms will increase, because the users will likely not receive training on how to use their system.

**2. Allowing direct connection of all IP enable alarm devices to the PSAP would expose public safety to "autodialer" problems.**

Society has already experienced the aggravation and drain on resources that can be caused by automated devices: Spam, junk mail, auto-dial solicitations, and mass-

emailed computer viruses have all disrupted daily life and wasted untold resources. If home-made or off the shelf alarm devices are allowed to send alarm signals directly to the PSAP without screening, PSAPs could be bombarded over and over with automatically sent signals and messages that could overwhelm their ability to receive legitimate emergency calls. Hundreds, thousands or tens of thousands of false alarms could be sent by a single device, either maliciously or due to a malfunction or improper programming of the device causing an autodialer situation.

### 3. False Signals Could Effectively Shut Down PSAPs, if Unscreened Alarm Signaling is Allowed.

The outcome of all of the above issues associated with direct alarm signaling is obvious: Each PSAP's ability to receive and process 911 calls/messages will lag, in most cases significantly. Legitimate calls will be put on hold for an unacceptably long time (as already happens in the event of bad storms and other emergencies). In essence, every day will be like the 2010 blizzard or September 11, 2001, with PSAPs being so overwhelmed that calls go unanswered. It will be difficult to address this issue by simply hiring more PSAP dispatchers. PSAP personnel are specially trained at significant expense to state and local governments, being certified by the Association of Public-Safety Communications Officials (APCO). See, e.g., Prince William County, Virginia 9-1-1 Center FAQs at p. 2.[6] At a time when state and local governments are being forced to cut public safety budgets because of the recession,[7] it will be difficult to find funds to double

[6] http://pwcgov.org/default.aspx?topic=040075000670000399.

[7] *See, e.g.*, "Legislators Warned State Budget Cuts Could Hurt Public Safety", the Wichita Eagle, February 19, 2011; "East Lansing's Public Safety to be Hurt by Governor Snyder's Cuts", Nathan Triplett, LSJ.com, February 27, 2011; "Schools, Healthcare, Public Safety Lose Millions in Va. Budget", Washington Post, March 15, 2010; "SD Police Chief: Budget Cuts Could Threaten Public Safety", 10news.com, October 7, 2010.

or triple the number of specially trained operators, especially when these operators will be spending most of their time screening false signals. Aside from the inability of PSAPs to handle the volume of false 911 messages, state and local will then waste untold resources dispatching scarce police, fire and rescue personnel to investigate 911 calls/signals that cannot be definitely ruled out as an emergency. As a result, the response to genuine emergencies will be slowed, resulting in loss of life and severe impacts on entire communities (especially in the case of fires, floods and other widespread crises); and the budgets for police and fire departments will have to be tripled or quadrupled. It is entirely possible that the volume of false 911 calls could effectively shut down many PSAPs for significant stretches of time. Because of these dangers, there are currently hundreds of local ordinances prohibiting the direct connection of automatic devices to the 911 system. Attachment A hereto contains examples of such ordinances from communities such as Lincoln, Nebraska and El Cerrito, California. If PSAPs are now subjected to an outrageous volume of unscreened alarm calls, it may very well result in the immediate and unilateral withdrawal of alarm response by law enforcement across this country.

### C. Direct Alarm Signaling Can Significantly Increase Liability for PSAPs, Since They Lack a Contractual Relationship With the Callers.

If the general public is allowed to send unscreened alarm signals from a variety of devices directly to the PSAP, it can place state and local governments and their employees into a murky situation where they can be sued, and perhaps held liable for any harm that may arise from a situation embodied in the sending of an alarm signal. More and more, courts are ruling that governments and their employees can be sued for a botched emergency response. See, e.g., "N.J. Appeals Court Rules 911 Operators Can Be

Sued For Mistakes", Mary Ann Spoto, the Star-Ledger, August 4, 2010. At a time when there would be an overwhelming increase in the number of 911 calls due to direct alarm signaling ability, PSAP personnel would suddenly be required to investigate every nuance of each signal sent to the PSAP, generally without the benefit of a human being to question about the situation. In essence, PSAP personnel will be required to undertake the screening process now performed by central stations, but without the background information and multiple contact numbers developed by central stations through their contractual relationship with their customers. And if an alarm signal of uncertain origin and nature is not instantly responded to and it turns out to be an actual emergency, the PSAP and/or operator may face a lawsuit. Unlike a central station alarm company, the PSAP would not have a contractual arrangement with the sender of the alarm signal that clearly spells out the protocol that will be followed if, e.g., the alarm signal is sent but the operator is unable to reach a human to verify that the alarm is genuine.

### D. The Proposal to Allow Security Cameras to Directly Contact a PSAP Raises Even More Issues.

As noted above, Paragraph 58 of the NOI poses the question of whether the Commission should facilitate automatic 911 calls by security cameras. This proposal raises all of the issues discussed above, as well as another difficult issue: If a PSAP receives raw camera footage from a security camera, how is the PSAP operator to interpret the footage? If the operator sees a person approaching the front door of a residence, is it an intruder, or the paperboy trying to collect his bill? Or perhaps it is a homeowner who forgot his or her keys? If a raccoon is seen approaching the house, can the operator assume that this can be ignored? Or if it turns out that the raccoon had rabies and bites the homeowner's child, will the PSAP and the operator be held liable for not

dispatching animal control? PSAPs cannot devote staff to stare at raw camera footage and interpret events. Moreover, what if the image is grainy or too dark? A wide variety of security cameras are available from "box stores", including very inexpensive but lesser quality cameras.[8] And public safety agencies cannot afford to send an emergency response every time a suspicious but blurry image sent by a security camera appears on a screen.

### E. PSAPs Should Not Be Bombarded with 911 Signals from Televisions, iPods and Gaming Consoles.

Paragraph 52 of the NOI asks whether every consumer device with IP communications capabilities should be able to contact a PSAP, even iPods and gaming consoles:

> Currently, only devices that provide telephone services are capable of transmitting 911 calls. In the future, however, most electronic devices will have communication capabilities, ranging from televisions, in-car systems, portable music players, tablet computers, and game consoles. *We seek comment on what devices can usefully provide emergency calling services. Should every consumer device with Internet or cellular connectivity and a suitable user interface have the ability to request emergency assistance? [Emphasis added]*

It is respectfully submitted that allowing the sending of 911 calls from such consumer devices will create far more issues that benefits. A large percentage of persons operating televisions, portable music players, game consoles and a number of other entertainment devices are children. While there is a chance that a legitimate emergency could be reported using one of these devices, there is also a significant probability that numerous bogus 911 calls would be placed, often by minors that may think the 911 button is to summon

---

[8] See, e.g., the following link: http://www.samsclub.com/sams/shop/category.jsp?categoryId=9143&navAction=jump&iid=Header|All_Pr

help because, e.g., the video game screen froze. And even many adults have had the experience of trying to use the 100 buttons that came on their television remote, only to find that they have accidentally programmed the television so that all shows are in Spanish or French. It will be counterproductive if it becomes possible to accidently make a 911 call when trying to program a VCR or find the channel guide.

## III. The Commission Should Find That, on Balance, Direct 911 Calls From Consumer Alarm Systems, Security Cameras and Entertainment Devices Should Not be Allowed.

Paragraph 49 recognizes that PSAPs "could face operational and funding burdens", and asks for comment on "tradeoffs", strengths and weaknesses:

> [W]hile application of IP-based approaches has generally led to robust and unexpected innovations in communications technologies, PSAPs could face operational and funding burdens from supporting a large number of IP-based NG911 architectures, and resources could be diverted from technical solutions that incorporate standardized features and implementation approaches. Similarly, introduction of operational requirements such as reliability, scalability, and standardized technology could result in tradeoffs between various legacy, proprietary, end-to-end open-standard, or other approaches for IP-based NG911 systems. *We request that commenters identify these tradeoffs, or other relevant tradeoffs, and discuss the relative strengths and weaknesses of these technical approaches. [Emphasis added]*

Because of the issues described above, it is respectfully submitted that allowing direct 911 calls from consumer alarm devices, security cameras and entertainment devices will, on balance, place a far greater burden on PSAPs and first responders than

---

oducts|Security Cameras

any benefits that would be garnered. The Commission should recognize that this tradeoff would ultimately be more harmful to consumers than beneficial, and shape its Next Generation 911 rules accordingly.

**Conclusion**

AICC encourages the Commission to modify its proposed NG 911 rules to allow E911 calls using technologies where a high degree of adult human interaction prevents the sending of false, inadvertent, automated or malicious emergency calls. The Commission should specifically refrain from facilitating the sending of alarm signals directly from alarm devices, security cameras and entertainment devices to the PSAP. Instead, the Commission should preserve the current arrangement whereby trained central station personnel screen alarm signals, to prevent a flood of false alarms to the already-overburdened PSAPs.

Respectfully submitted,

**Alarm Industry Communications Committee**

By: /s/_____
John A. Prendergast
Its Attorney

Blooston, Mordkofsky, Dickens,
Duffy, & Prendergast, LLP
2120 L Street NW
Suite 300
Washington DC 20037
Tel: 202-659-0830

Dated: February 28, 2011

## ATTACHMENT A

## EXCERPTS OF EXAMPLES OF LOCAL ORDINANCES PROHIBITING DIRECT CONNECTION OF AUTOMATIC ALARM DEVICES TO 911

### El Cerrito Municipal Code (California)

### CHAPTER 6.55 ("ALARM SYSTEMS")

**Sec. 6.55.070 Alarm Systems: Prohibited systems**

No Alarm User shall Permit the installation or use of and no Alarm Business shall install:

(a) An Alarm System with a direct dial to the police department of the City of El Cerrito; or

(b) An Alarm System, which contains components that are not UL (Underwriters' Laboratory) listed or the equivalent.

### Vallejo Municipal Code (California)

### CHAPTER 7.81 SECURITY ALARM SYSTEMS

**7.81.50 Features and interconnection.**

C. No automatic dialing device shall be interconnected to dial the 9-1-1 operator or any telephone number of the Vallejo Police Department. Any person who knowingly interconnects or permits such interconnection of an automatic dialing device is guilty of an infraction as provided in the ordinance codified in this chapter.

# Lincoln Municipal Code (Nebraska)

## CHAPTER 5.56 EMERGENCY ALARM SYSTEMS

### 5.56.060 Automatic Dialing Devices

(a) Except as otherwise provided in this chapter, no automatic dialing device shall be interconnected to any trunkline, terminating in the emergency communications center.

(b) Within ninety days after the effective date of this ordinance, all automatic dialing devices interconnected to a primary trunkline shall be disconnected therefrom. The owner or lessee of such device shall be responsible for having the device disconnected within the ninety day time period.

(c) Persons owning or leasing an automatic dialing device may have the device interconnected to a telephone line transmitted directly to:

(1) a central station;

(2) an answering service;

(3) automatic dialing devices may also be interconnected to one or more telephone numbers available to the owner or lessee of the devices, or their designated representatives, at another location. (Ord. 15482 §6; March 5, 1990: P.C. §5.15.060: Ord. 13438 §6; August 30, 1982).

**Service List**

Julius Genachowski, Chairman
Federal Communications Commission
445 12th Street SW, Room 8-B201
Washington, DC 20554
E-Mail: julius.genachowski@fcc.gov

Michael J. Copps, Commissioner
Federal Communications Commission
445 12th Street SW, Room 8-B115
Washington, DC 20554
E-Mail: michael.copps@fcc.gov

Robert M. McDowell, Commissioner
Federal Communications Commission
445 12th Street SW, Room 8-C302
Washington, DC 20554
E-Mail: robert.mcdowell@fcc.gov

Mignon Clyburn, Commissioner
Federal Communications Commission
445 12th Street SW, Room 8-A302
Washington, DC 20554
E-Mail: mignon.clyburn@fcc.gov

Meredith Attwell Baker, Commissioner
Federal Communications Commission
445 12th Street SW, Room 8-A204
Washington, DC 20554
E-Mail: MeredithAttwell.Baker@fcc.gov

Rick Kaplan
Legal Advisor to Chairman Genachowski
445 12th Street SW, Room 8-B201
Washington, DC 20554
E-Mail: rick.kaplan@fcc.gov

John Giusti
Legal Advisor to Commissioner Copps
445 12th Street SW, Room 8-B115
Washington, DC 20554
E-Mail: john.giusti@fcc.gov

Angela Giancarlo
Legal Advisor to Commissioner
McDowell
445 12th Street SW, Room 8-C302
Washington, DC 20554
E-Mail: angela.giancarlo@fcc.gov

Louis Peraertz
Legal Advisor to Commissioner Clyburn
445 12th Street SW, Room 8-A302
Washington, DC 20554
E-Mail: louis.peraertz@fcc.gov

Charles Mathias
Legal Advisor to Commissioner Baker
445 12th Street SW, Room 8-A204
Washington, DC 20554
E-Mail: charles.mathias@fcc.gov

Best Copy and Printing, Inc. (BCPI)
Portals II
445 12th Street, S.W., Room CY-B402,
Washington, D.C. 20554
Email: fcc@bcpiweb.com